A DECISION MAKING MODEL FOR SECURELY CONDUCTING ELECTRONIC COMMERCE

Alexander D. Korzyk, Sr, Virginia Commonwealth University
J. G. VanDyke & Associates
4738 Cedar Cliff Road
Chester VA 23831
804.748.8590
Internet address: akorzyk@acm.org

ABSTRACT

The small to medium size enterprise faces many problems not faced by larger enterprises. One of these important problems in today's Internet World is how to establish a presence on the Internet and securely conduct electronic commerce. Large enterprises have much greater resources and usually include the development and execution of their Internet strategy in the Information Services Division. Unfortunately, most small to medium sized enterprises have a very small information technology staff if they have an information technology staff at all. Faced with the dilemma of hiring a new information technology Internet specialist, training the current Information Analyst, or contracting out the Internet business requirement, management must make a hard decision. Perhaps the most critical criteria in determining which alternative to choose are maximizing security and minimizing financial losses due to computer security incidents. The average loss of a computer security incident for all sizes of business is over $100,000 (Ban and Heng 95). The damage to the company's mission critical application could possibly result in bankruptcy or significant damage for a small to medium size enterprise. With the great increase in the number of businesses making a presence on the Internet and the increase in the number of cyber-customers, the chances of a computer security incident increases daily. Should a small to medium sized enterprise attempt to establish and maintain their presence on the Internet with internal assets or should they contract the Internet requirement? This paper researches the factors of this decision faced by management and quantifies the decision making process to justify a business case for how to establish and maintain a secure Internet presence.

INTRODUCTION

There are literally millions of small to medium enterprises that want to conduct business on the World Wide Web but are afraid to do so because of the lack of security in their infrastructure and information systems (Row 97). Unlike corporations and large organizations that for several years and in some cases decades, operated in isolation on their own private networks, the small to medium enterprises struggled with little or no automation until the invention of the personal computer. Most small to medium enterprises could not afford the capital investment necessary to establish an infrastructure to support business operations. Many of these small to medium enterprises even leased hardware and software because they could not afford to refresh their technology if they outright purchased the hardware and software because it became obsolete in three years. Now as budget cuts have become commonplace and organizations want to get on the World Wide Web without compromising information security, everyone's information becomes available to everyone else if it is not protected properly. In Australia, small to medium sized enterprises are much more numerous than large corporations (96% of all corporations) and employ 56% of the private sector (Goldsworthy 97). Corporations have not fully embraced Electronic Commerce/Electronic Data Interchange (EC/EDI) (Borg 97). The Federal, state, and local governments and corporations have again been hesitant to implement EC/EDI because of the lack of security technology used on the Internet and World Wide Web (Power 97). The governments

and corporations also want to use the Web as the infrastructure on which to run EC/EDI. But what about the small to medium enterprises that also want to conduct electronic commerce securely?

Many small companies wish to have the opportunity to expand should new business become available. One of the problems that most small companies face is how to afford getting new business? Preparing cost proposals take up much time and resources with a small chance of getting the new business. Advertising in local papers may have gotten only a handful of responses. Current business may have been obtained by personal networking. The trend for many small companies is to now advertise on the WWW just like the large companies. With key word searches, not only will the big corporations appear in the prospects search but small companies would also appear. Perhaps some local firms may be willing to do business with a small company and possibly get a better product faster than with a large company and possibly get a worse product.

The WWW could give companies the capability to transfer files and documents for a low monthly unlimited access fee to the WWW. The majority of data transfer in small companies is currently done by dialing up point to point and paying for each minute of phone line usage or by snail mail (the term for regular postage mail). The web would also allow access to the company public database for product information. One course of action would be to outsource a web page from companies that specialize in running web servers. This Internet service provider would be responsible for making sure that the web server was secure. The Internet solution provider should use a firewall and other web security products to greatly reduce the chances of an attack from both the outside and inside of the small to medium enterprise. The Internet service provider would pay for the expensive software that may be required to secure the web server. A second course of action would be for the company to purchase, set up, and maintain their own web server. The company would bear the expense of securing the web server. They would still have to support non-web users as well. This course of action would require a decision between the company hiring an Internet specialist to set up their own web server or train a current Information technology specialist to set up their own web server. The chance of losing data or suffering a financial loss due to an outside attack increases dramatically with the personnel lack of security expertise.

RESEARCH QUESTION

The primary purpose of this research was to develop a decision making model for how to conduct business on the Web based on security threats. The research question concerning businesses included the following:

> Should a small to medium enterprise outsource to securely conduct electronic commerce based on security threats?
>
> Should the enterprise hire an Internet specialist to securely conduct electronic commerce based on security threats?
>
> Should the enterprise train a current Information technology specialist to securely conduct electronic commerce based on security threats?

RESEARCH METHODS

This research uses decision analysis methodology to develop a decision making model for how to securely conduct electronic commerce based on security threats was to follow decision analysis methodology. Many small to medium enterprises cannot afford to even develop a business case for conducting business on the Web or they may even know the options available to them. This

research will enable any small to medium enterprise to decide if they should outsource their Internet business or attempt to conduct their Internet business internally with a new hire or by training a current employee.

Fundamental Objectives Hierarchy

The fundamental objectives hierarchy structures the values of the small to medium enterprise. The manager of the small to medium enterprise wants to maximize profits but the manager wants to do so by minimizing the amount spent on computer and information security while maximizing the amount of computer and information security the enterprise receives. In this model the tradeoff is shown in Figure 1.

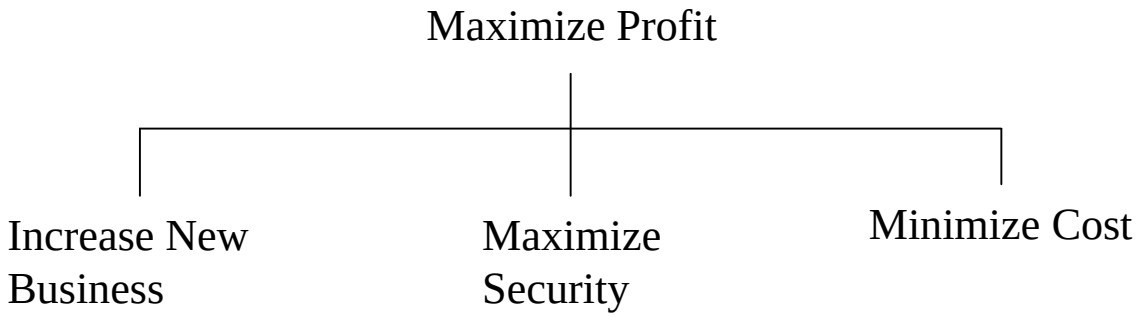


Figure 1—Secure Electronic Commerce Fundamental Objectives Hierarchy

Means Objectives Hierarchy

The means objectives hierarchy separates the means from the fundamental objectives within the decision context (Clemen 96). Each means objectives helps accomplish a sub-objective while the fundamental objectives are just important. Figure 2 contains the means objectives hierarchy for the model.

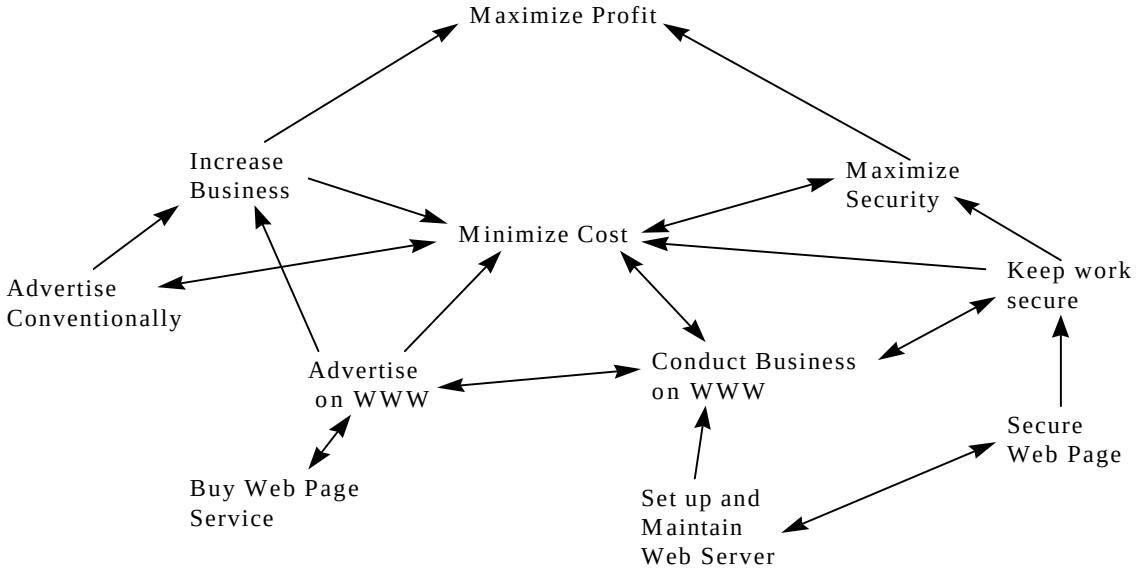


Figure 2—Secure Electronic Commerce Means Objective Hierarchy

Influence Diagram

The influence diagram to represent this decision in Figure 3 contains chance nodes in the ovals, mathematical calculation or consequence nodes in the rounded rectangles, and decision modes in the rectangle.

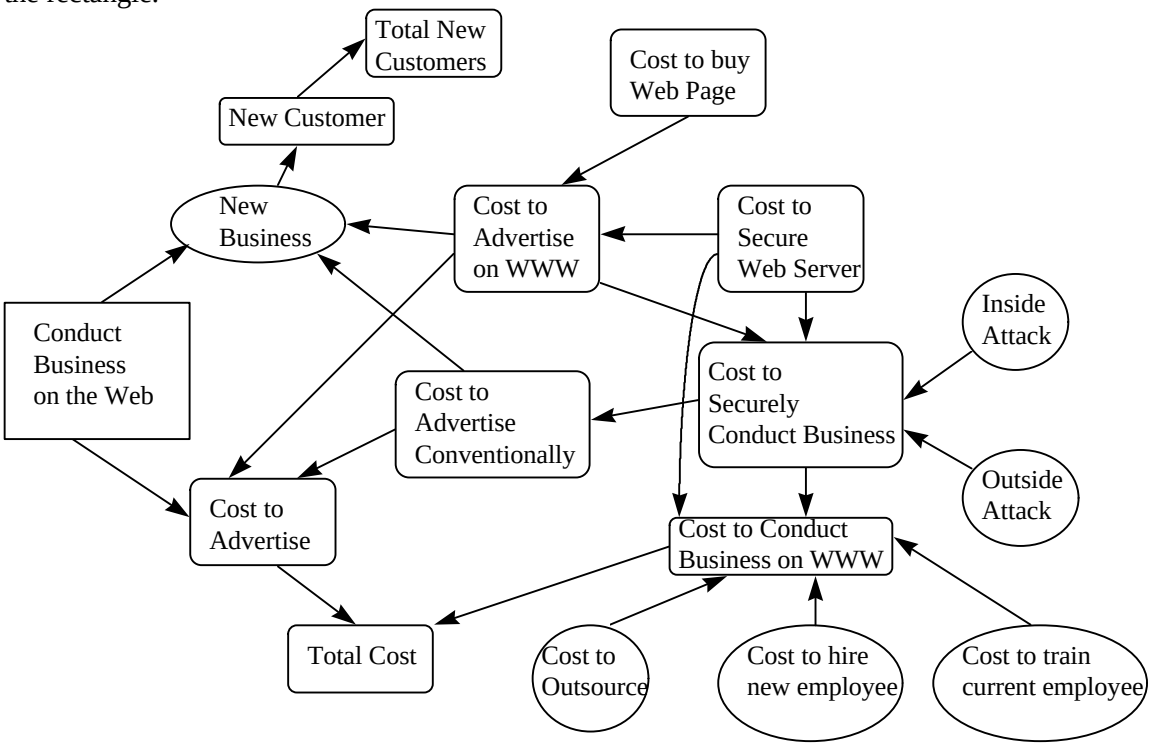


Figure 3—Secure Electronic Commerce Security Influence Diagram

Evaluation Criteria

This paper examined the decision facing more and more businesses both old and new around the world each year. The number of all companies conducting financial business on the Internet has doubled in one year. Since 1995, the number of companies buying goods and materials on the Internet has increased from 6 to 14%; the number of companies selling goods and materials on the Internet has increased from 5 to 9% (Wilder and Kolbasuk McGee 97). Small and medium sized enterprises compared to larger organizations who have full time assets devoted to computer security lack personnel and resources for a full time asset. The Information manager is presumed to shoulder this role as part of his job responsibility (Ban and Heng 95). Can the small to medium enterprise afford to not outsource Internet operations based on security threats?

The decision of whether to outsource web business or to conduct web business with internal resources from the computer security context needs objective evaluation criteria. Further, the paper examines conducting web business with a new employee with Internet skills or training a current employee. The fundamental objectives hierarchy identified three sub objectives to the prime objective of maximizing profit. These are increasing revenue (new business), maximizing computer security, and minimizing cost. Decision analysis methodology states that we would like to measure the available alternatives relative to the fundamental objectives (Clemen 96). The attribute for the objective to minimize costs will be measured in dollars. This model will not measure the attribute for the objective increase revenue (new business). The attribute for maximizing computer security will be measured indirectly by constructing a probability matrix for the probability of an inside computer attacks and the probability of an outside computer attacks

and multiplying that probability by the average financial loss for the type of attack by the size of the enterprise. From the computer security context, minimizing costs will involve deciding between outsourcing Internet support or trying to build and successfully use internal Internet support. For example, in the Richmond area, there are several sources which provide Internet service. One provides web site design, hosting, and access consultation for $19.95 per month. Another provides advertising on the Internet for $25 per month. Another provides high speed Internet access, web site design, and web hosting for varied amounts up to $80.00 per month for a non-virtual Internet address. One advertises that it provides interactive net-based business solutions, designing web sites and providing secure hosting and superior access services for an unadvertised amount. Two advertise that they provide complete turnkey web sites at an unadvertised amount. Another offers web site development, web access and networking services for an unadvertised amount. While another advertises that it provides a free web page, and technical support for only $10 per month. One advertised that their pages get noticed for an unadvertised amount. These very low advertised amounts normally do not include any Internet on-line ordering or selling capability. The author was unable to determine at this time if these Internet Providers would guarantee against financial loss due to an attack by an outsider or insider. There have been several recent articles citing the unreliability of Internet providers. The alternative for outsourcing is to provide your own web host. Companies such as **Video Direct Corporation** advertises that you do not need a computer or training. They advertise that for $39.95 you receive their business manual & forms, ad slicks & press releases, instant use of their Internet catalog, and regular Internet web site updates to become an independent consultant promoting their catalog. **MacGraw-Hill Internet Training Manual** gives the user a step-by-step instructional guide to building and running a business on the web for $32.95. MacGraw-Hill also publishes **Making More Money on the Internet** by Emily Glossbrenner to help your business begin to sell products or services including guidelines for encryption and security.

The first criterion of maximizing security is addressed by the quantitative variable of the financial loss associated with the attack on the information system. The financial loss is independent of whether the attack came from within the company or outside the company. An Ernst and Young survey of all size enterprises conducted in 1996 (Violino 96), revealed that companies attacked had a probability of .05 for a financial loss of over $1,000,000 per attack; companies attacked had a probability of .25 for a financial loss of over $250,000 per attack; and the remaining companies had a probability of .7 for an undetermined amount of financial loss. The Ernst and Young survey further discovered that financial losses come from several causes listed in Table 1 (Violino 96).

Security Problem resulting in financial losses sited above.	Probability of companies with loss from this security problem (independent).
Industrial espionage	.09
Attacks from outside the company	.23
Natural disasters	.29
Attacks from inside the company	.41
Downtime from non-disasters	.6
Accidental errors	.72
Computer viruses	.75
Unknown sources	.2

Table 1--Probability of Financial Losses

This paper focused on two of the security problems caused by the Internet dealing with attacks. The Attacks from outside the company has a probability of .23 and the attacks from inside the

company has a probability of .41. Another source sited the estimates for inside attacks as high as .80 back in 1991 (Bresnahan 97). Government agencies and organizations experience only .54 probability of an inside attack costing the government about $72,000 for each security incident (Power 97). For purposes of this research a virus was considered as part of an attack. The chances of contracting a virus is much greater on the Internet because of the high volume of users and traffic. Thus, an alternative without considering the threats of computer attacks must reflect the amount of financial loss associated with such an attack.

The second criterion for minimizing costs will be measured in terms of cost and cost avoidance. Based on the probabilities associated with different types of attacks, the company must plan on financial losses due to attacks. An alternative with high security capabilities will cost more in terms of initial outlay of capital but cost much less in terms of cost avoidance by preventing attacks from penetrating the enterprise computers. Measuring cost must include cost avoidance values in dollars using the probabilities in Table 1. The type of financial loss must be determined during a risk analysis of the company.

The priority of the criteria are:

1) Minimize Cost of conducting business on the Internet;
2) Maximize security.

The minimum satisfaction level acceptable for each criteria are:

1) Minimize cost by choosing the optimal alternative for conducting business on the Internet.
2) Maximize cost by choosing the optimal alternative for conducting business on the Internet that reduces the chance of both inside and outside attacks.

QUANTITATIVE DATA ANALYSIS

The software tools used to conduct the quantitative data analysis were Microsoft Excel version 6.0 and Treeplan add-in for Excel 6.0.

Decision Trees

In order to evaluate the three alternatives, the author developed a model decision tree using Excel and the Treeplan add-in. The model decision tree allows any enterprise or organization to enter values into the parameters to determine if the enterprise or organization should outsource conducting business on the Internet.

Model Decision Tree

There are three decision nodes contained in the model. One sub-branch contains two decision sub-trees. One sub-tree outsources most of the Internet business services required outside the enterprise or organization to a specialty company and the second sub-tree keeps the service internal to the enterprise but provides a decision on whether to train a current employee or hire a new employee with Internet expertise. The associated financial loss in dollars with the size of the enterprise and general probabilities associated with the event nodes are contained in the table 2. The amount of financial loss is estimated based on various figures obtained from a review of the literature. The rational for the doubling of the amount of an inside attack versus an outside attack

is that the outside attacker is more likely to be committed with malicious intent (Bresnahan 97). The inside attack also could be committed with malicious intent but the majority of the inside security incidences are accidental versus intentional (Bernstein 97). Each of the Excel worksheets following the model use one set of data from table 2 depending on the size of the enterprise.

Security Incidents	Small Company Loss per attack	Medium Company Loss per attack	Large Company Loss per attack	Corporation Loss per attack
Inside Attack	10,000	50,000	100,000	1,000,000
Outside Attack	20,000	100,000	200,000	2,000,000

Table 2. Financial Loss by Type of Attack and Size of Enterprise

The probabilities in the model come from the table 3. Outsourcing to a reputable Internet Provider which has high security capabilities increases the chances that no attack will occur, thus reducing the chance of an outside attack and slightly reducing the chance of an inside attack. On the other hand outsourcing to an irreputable Internet Provider could raise risks (Caldwell 97). Hiring an Internet specialist may also increase the chances that no attack will occur but the enterprise hiring the Internet specialist may not have the capital to purchase the necessary security software to adequately protect the enterprise. Thus the chances of an outside attack are still higher than outsourcing but less likely than training a current employee. The chance of an inside attack remains the same since the Internet specialist is primarily concerned with outside the enterprise. Training a current employee poses the most risk of a successful outside attack. Although the employee may be very proficient in their current position, the chances are that within the first year something will happen that the employee just did not realize was possible because of lack of knowledge. Thus, the probability of no attack is very small compared to the probability of an outside attack, while the probability of an inside attack remains the same.

Decision	Inside Attack	Outside Attack	No Attack
Outsource	.33	.33	.33
Internal Hire	.4	.4	.2
Internal Train	.4	.5	.1

Table 3. Probabilities of Attacks by Type of Attack by Decision

Using the information provided by Table 3, the model is constructed. The information from Table 2 provides data for the four decision trees that follow the model decision tree.

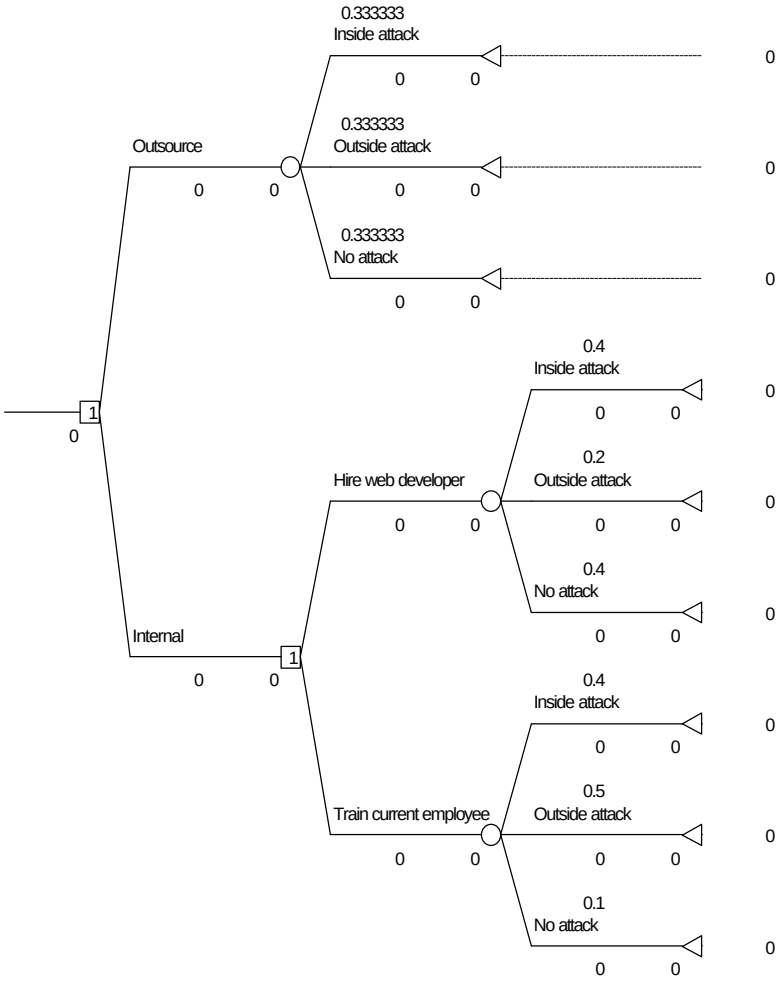


Figure 4—Secure Electronic Commerce Decision Model

Corporation

This section considers the corporation as an enterprise grossing over $100,000,000 revenue per year. Not surprisingly, the optimal solution for the corporation is to keep the function internal to the company. However, the optimal solution for how to keep the Internet function in the company is to hire an Internet specialist rather than try to train a current employee and face additional risks. The costs for an Internet web developer is estimated at an industry average of $70,000 per year in the United States. The costs for training a current employee in web development, web security, etc. is approximately $30,000. This cost of training is in addition to a base salary industry average of $60,000 per year in the United States. The Outsource alternative incurred a cost of $36,000 per year based on using various services from the Internet Service Provider with the capability to handle electronic commerce, secured with a firewall, and dynamic web page development costing approximately $2,000 per month. The web hardware platform, maintenance support, and telecommunications charges cost approximately $1,000 per month. These figures were compiled from a recent market survey conducted by the author.

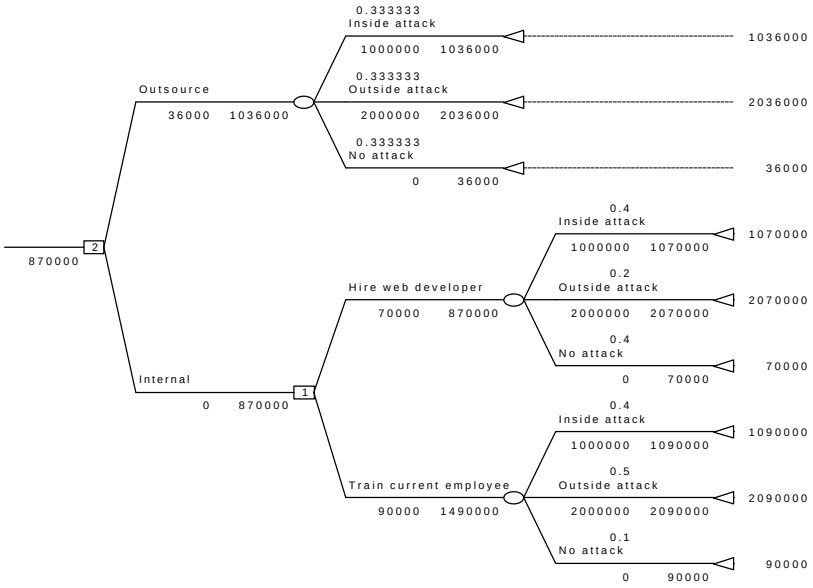


Figure 5--Corporate Secure Electronic Commerce Decision Model

Large Enterprise

This section considers a large enterprise as one grossing between one million and one hundred million dollars per year. The optimal decision for the large enterprise is to outsource the Internet requirement. The costs for an Internet web developer is estimated at an industry average of $70,000 per year in the United States. The costs for training a current employee in web development, web security, etc. is approximately $30,000. This cost of training is in addition to a base salary industry average of $60,000 per year in the United States. The Outsource alternative incurred a cost of $36,000 per year based on using various services from the Internet Service Provider with the capability to handle electronic commerce, secured with a firewall, and dynamic web page development costing approximately $2,000 per month. The web hardware platform, maintenance support, and telecommunications charges cost approximately $1,000 per month. These figures were compiled from a recent market survey conducted by the author.

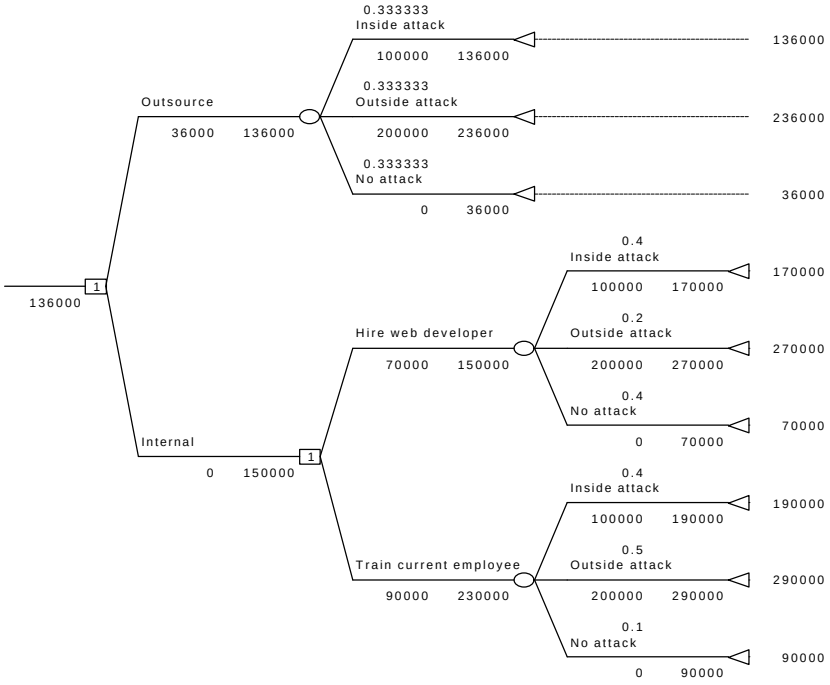


Figure 6--Large Enterprise Secure Electronic Commerce Decision Model

Medium Enterprise

This section considers a medium enterprise to have between two hundred fifty thousand dollars and one million dollars of gross revenue per year. The optimal alternative for the medium enterprise is to outsource the Internet requirement. The costs for an Internet web developer is estimated at an industry average of $70,000 per year in the United States. The costs for training a current employee in web development, web security, etc. is approximately $30,000. This cost of training is in addition to a base salary industry average of $60,000 per year in the United States. The Outsource alternative incurred a cost of $36,000 per year based on using various services from the Internet Service Provider with the capability to handle electronic commerce, secured with a firewall, and dynamic web page development costing approximately $2,000 per month. The web hardware platform, maintenance support, and telecommunications charges cost approximately $1,000 per month. These figures were compiled from a recent market survey conducted by the author.

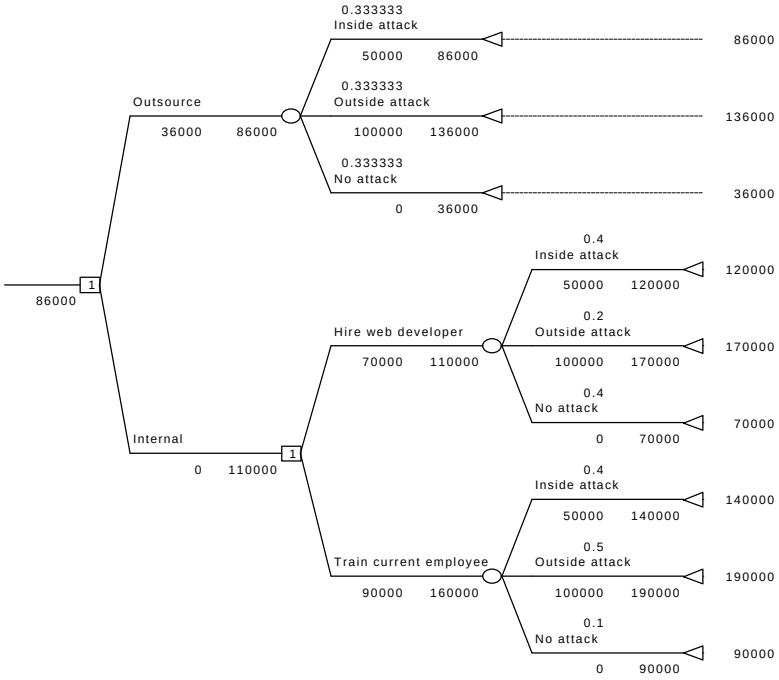


Figure 7--Medium Enterprise Secure Electronic Commerce Decision Model

Small Enterprise

This section considers a small enterprise to have less than two hundred fifty thousand dollars of gross revenue per year. The optimal alternative for the small enterprise is to outsource the Internet requirement. The costs for an Internet web developer is estimated at an industry average of $70,000 per year in the United States. The costs for training a current employee in web development, web security, etc. is approximately $30,000. This cost of training is in addition to a base salary industry average of $60,000 per year in the United States. The Outsource alternative incurred a cost of $36,000 per year based on using various services from the Internet Service Provider with the capability to handle electronic commerce, secured with a firewall, and dynamic web page development costing approximately $2,000 per month. The web hardware platform, maintenance support, and telecommunications charges cost approximately $1,000 per month. These figures were compiled from a recent market survey conducted by the author.

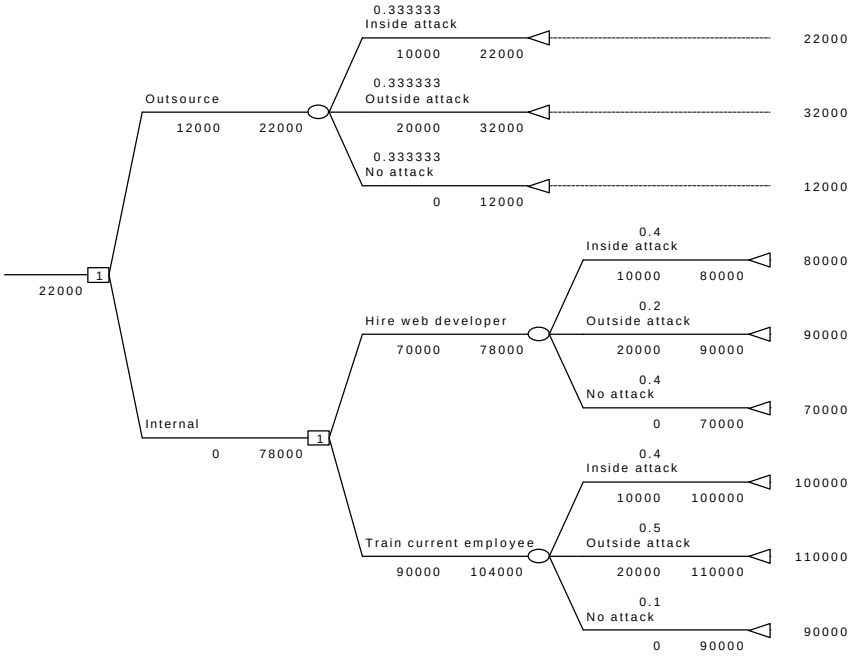


Figure 8--Small Enterprise Secure Electronic Commerce Decision Model

ATTITUDE TOWARDS RISK

Deterministically, neither alternative dominates the other. However, stochastically the outsourcing alternative dominates the other two alternatives using the figures from Table 3.

	Inside	Outside	No attack
Outsource	0.33	0.33	0.33
Hire	0.4	0.4	0.2
Train	0.4	0.5	0.1

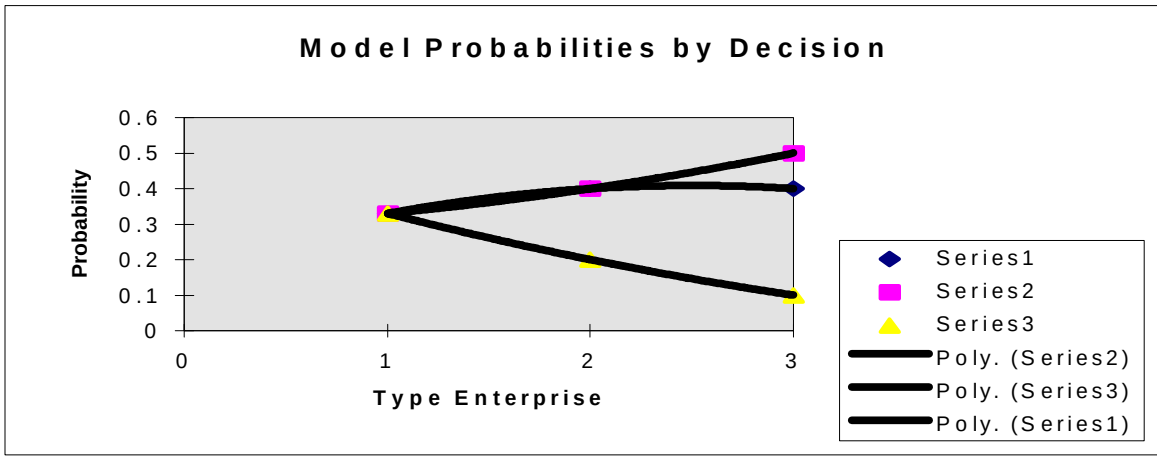


Figure 9—Stochastic Dominance

SENSITIVITY

The model is sensitive to the amount of expected financial loss. Although the corporation optimal decision is to keep the function in-house, a large or even medium enterprise with a high probability of a catastrophic loss above the amount in Table 3 would then suggest that the optimal decision for the large and medium enterprise would be to keep the Internet function in-house. Table 4 summarizes the results of the four general types of enterprises.

Size of Enterprise	Cost of Single Inside Attack	Expected Value (Outsource)	Expected Value (Hire)	Expected Value (Train)	Optimal Decision
Small	10,000	22,000	78,000	104,000	Outsource
Medium	50,000	86,000	110,000	160,000	Outsource
Large	100,000	136,000	150,000	230,000	Outsource
Corporate	1,000,000	1,036,000	870,000	1,490,000	Hire

Table 4. Secure Electronic Commerce Expected Value Matrix

RESULTS

The results of the data analysis with the Internet decision model clearly indicate that the optimal solution for the small to medium enterprise for securely conducting business on the Internet is to outsource the requirement rather than keep it in-house given the data in Table 2 and Table 3.

Further break-even analysis may be conducted by the user of the model by varying the probabilities in Table 3 and the financial loss for the type of attack in Table 2.

RECOMMENDATIONS FOR FURTHER RESEARCH

Further research using empirical data to validate the Secure Electronic Commerce decision model is needed. As more small to medium enterprises begin to conduct business on the Internet, researchers should conduct surveys specifically asking for the number of inside and outside attacks and the amount of financial loss associated with the type of attack.

REFERENCES

Ban, Lim Yew and Heng, Goh Moh, Computer Security Issues in Small and Medium-sized Enterprises, Singapore Management Review, Vol. 17, No. 1, Jan 1995, pp. 15-29.

Bernstein, David S., Infosecurity News industry survey, Infosecurity News, Vol. 8, No. 3, May 1997, pp. 20-27.

Borg, Kim, Web Readies Wares for Online "Shopholics" But security concerns keep them turned off, Computer Technology Review, Vol. 17, No. 3, March 1997, p. 1, 6-8.

Bresnahan, Jennifer, To Catch a Thief, CIO Magazine, March 1, 1997, pp. 68-72.

Caldwell, Bruce, Violino, Bob, and Kolbasuk McGee, Marianne, Hidden Partners, Hidden Dangers, Information Week, January 20, 1997, pp. 38-52.

Clemen, Robert T., Making Hard Decisions: An Introduction to Decision Analysis, 2nd edition, Duxbury Press at Wadsworth Publishing Company, New York, New York, 1996.

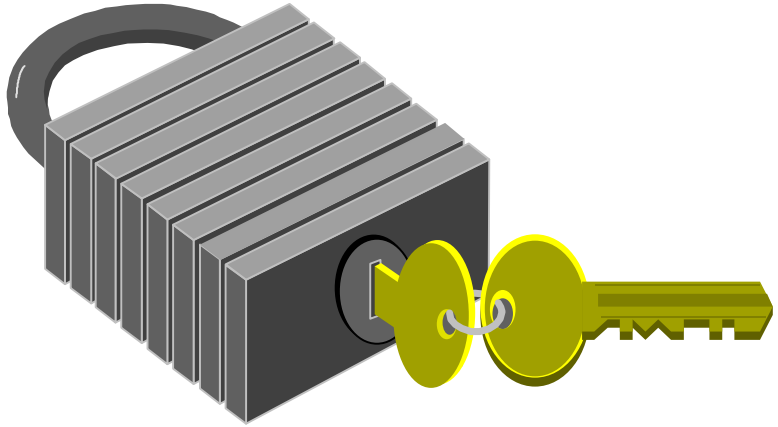
Goldsworthy, Mary-Anne, Electronic Commerce for Small to Medium Sized Enterprises, URL:http//www.arraydev.com/commerce/JIBC/9702-19.htm.

Power, Kevin, FBI finds hackers can't resist a government agency, Government Computing News, April 14, 1997, p. 60.

Row, Heath, The electric handshake, CIO Magazine, January 1, 1997, pp. 48-63.

Violino, Bob, The Security Facade, Information Week, October 21, 1996, pp. 36-48.

Wilder, Clinton and Kolbasuk McGee, Marianne, GE The Net Pays Off, January 27, 1997, pp. 14-16.



A Decision Making Model For Securely Conducting Electronic Commerce

by

Alexander D. Korzyk, Sr.

J. G. Van Dyke & Associates

Virginia Commonwealth University

Agenda

- CIO Top 10 Challenges
- CIO Top 10 Critical Techologies
- Research Questions
- SEC Fundamental Objectives Hierarchy
- SEC Means Objective Hierarchy
- SEC Influence Diagram
- Evaluation Criteria
- Quantitative Data Analysis
- Results
- Recommendations For Further Research

CIO Top 10 Challenges

Number By Rank	Challenge	Percent
1	**Implementing IT capital planning and investment management**	**76**
2	Measuring IT contribution to mission performance	56
3	**Formulating or implementing an agency IT architecture**	**52**
4	Aligning IT and organizational mission goals	41
5	Championing BPR as a precursor to IT decisions	37
6	Building effective relationships with agency senior executives	35
7	Gaining a seat at the senior management table	32
8	Engaging senior executives on IT strategic directions	30
9	Providing effective IT infrastructure and related services	27
10	Ensuring Year 2000 operations	25

Survey results from AFFIRM October 1996

CIO Top 10 Critical Technologies

Number By Rank	Critical Technology	Percent
1	Internet/Intranet/Web	73
2	**Security Technology**	**68**
3	Electronic Commerce/Electronic Data Interchange	57
4	Distributed Computing	47
5	Data Warehousing	42
6	Client/Server Computing	41
7	Workflow	35
8	Executive Information Systems/DS S	28
9	Groupware	22
10	Relational Databases	21

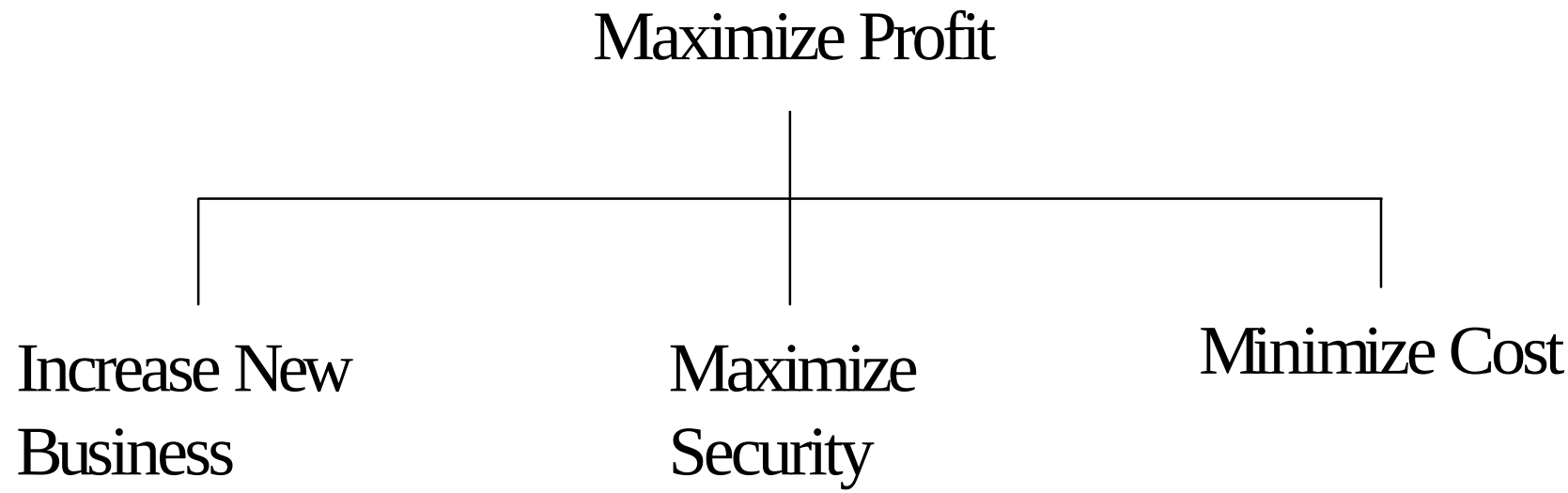
Survey results from AFFIRM June 1996

Research Questions:

Should a small to medium enterprise outsource to securely conduct electronic commerce based on security threats?

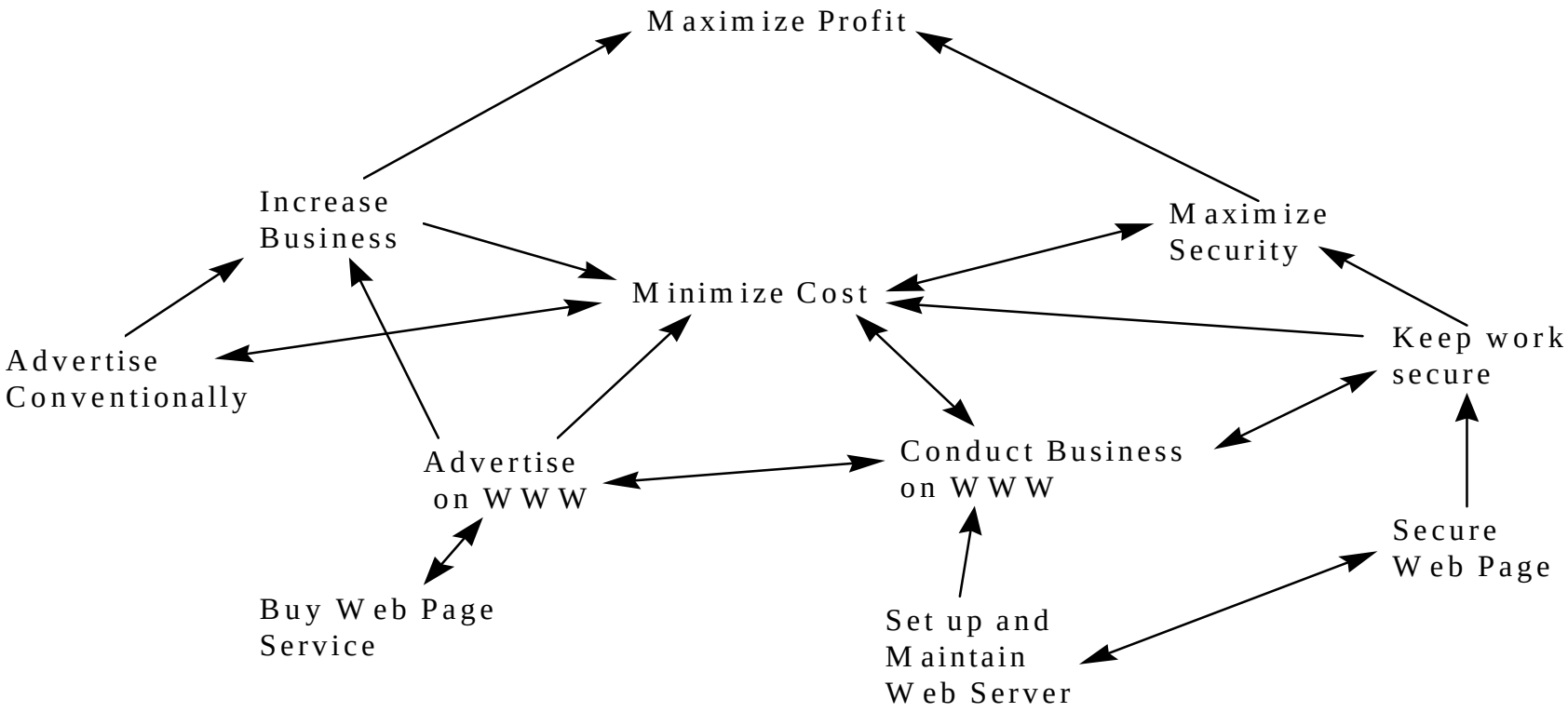
Should the enterprise hire an Internet specialist to securely conduct electronic commerce based on security threats?

Should the enterprise train a current Information technology specialist to securely conduct electronic commerce based on security threats?



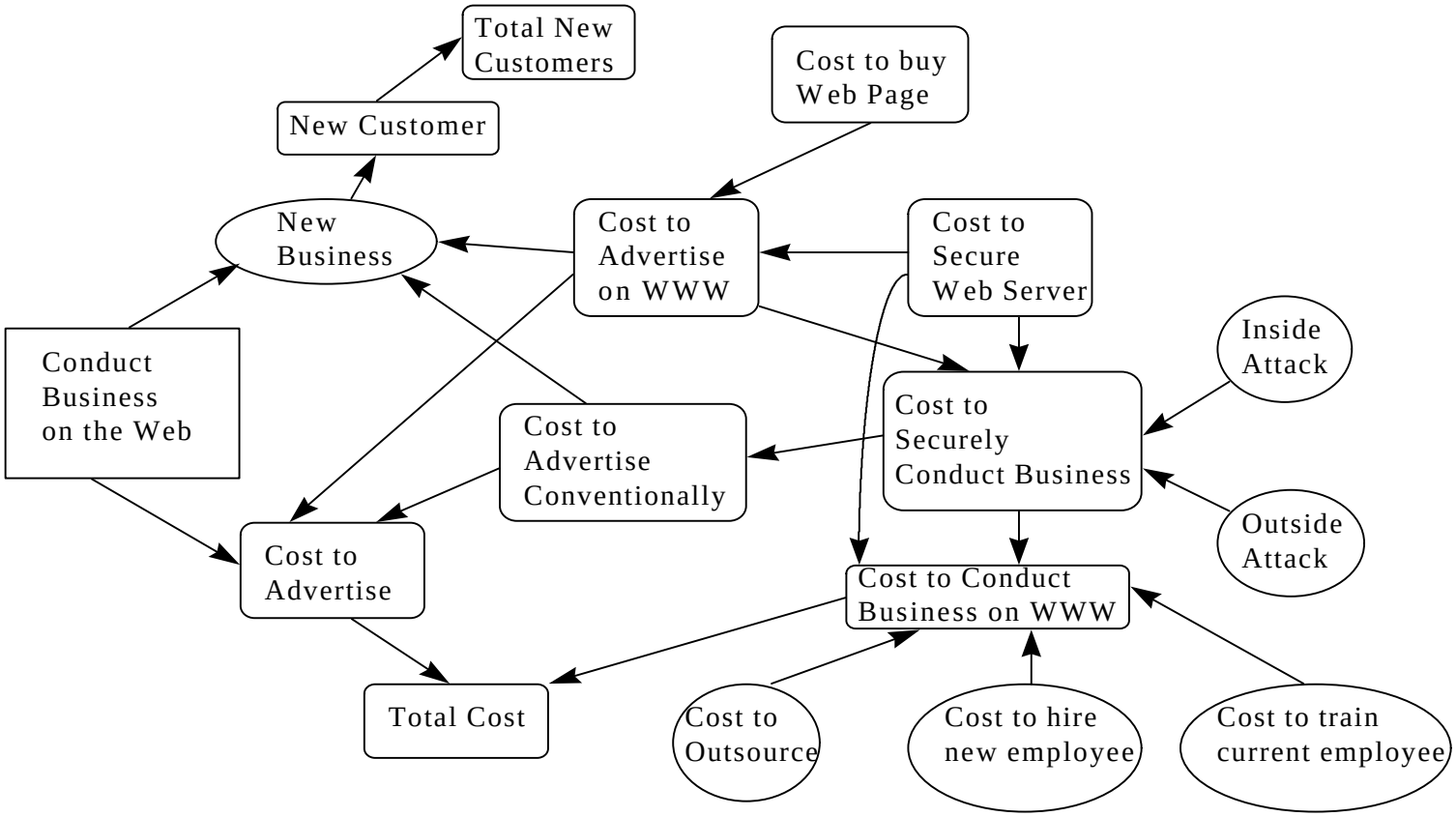
Secure Electronic Commerce Fundamental Objectives Hierarchy

A Decision Making Model for Securely Conducting Electronic Commerce



Secure Electronic Commerce Means Objective Hierarchy

A Decision Making Model for Securely Conducting Electronic Commerce



Secure Electronic Commerce Influence Diagram

Security Problem resulting in financial losses sited above.	Probability of companies with loss from this security problem (independent).
Industrial espionage	.09
Attacks from outside the company	.23
Natural disasters	.29
Attacks from inside the company	.41
Downtime from non-disasters	.6
Accidental errors	.72
Computer viruses	.75
Unknown sources	.2

Probability of Financial Losses (Violino, 96)

Evaluation Criteria

The priority of the criteria are:

1) Minimize Cost of conducting business on the Internet;
2) Maximize security.

The minimum satisfaction level acceptable for each criteria are:

1) Minimize cost by choosing the optimal alternative for conducting business on the Internet.
2) Maximize cost by choosing the optimal alternative for conducting business on the Internet that reduces the chance of both inside and outside attacks.

Security Incidents	Small Company Loss per attack	Medium Company Loss per attack	Large Company Loss per attack	Corporation Loss per attack
Inside Attack	10,000	50,000	100,000	1,000,000
Outside Attack	20,000	100,000	200,000	2,000,000

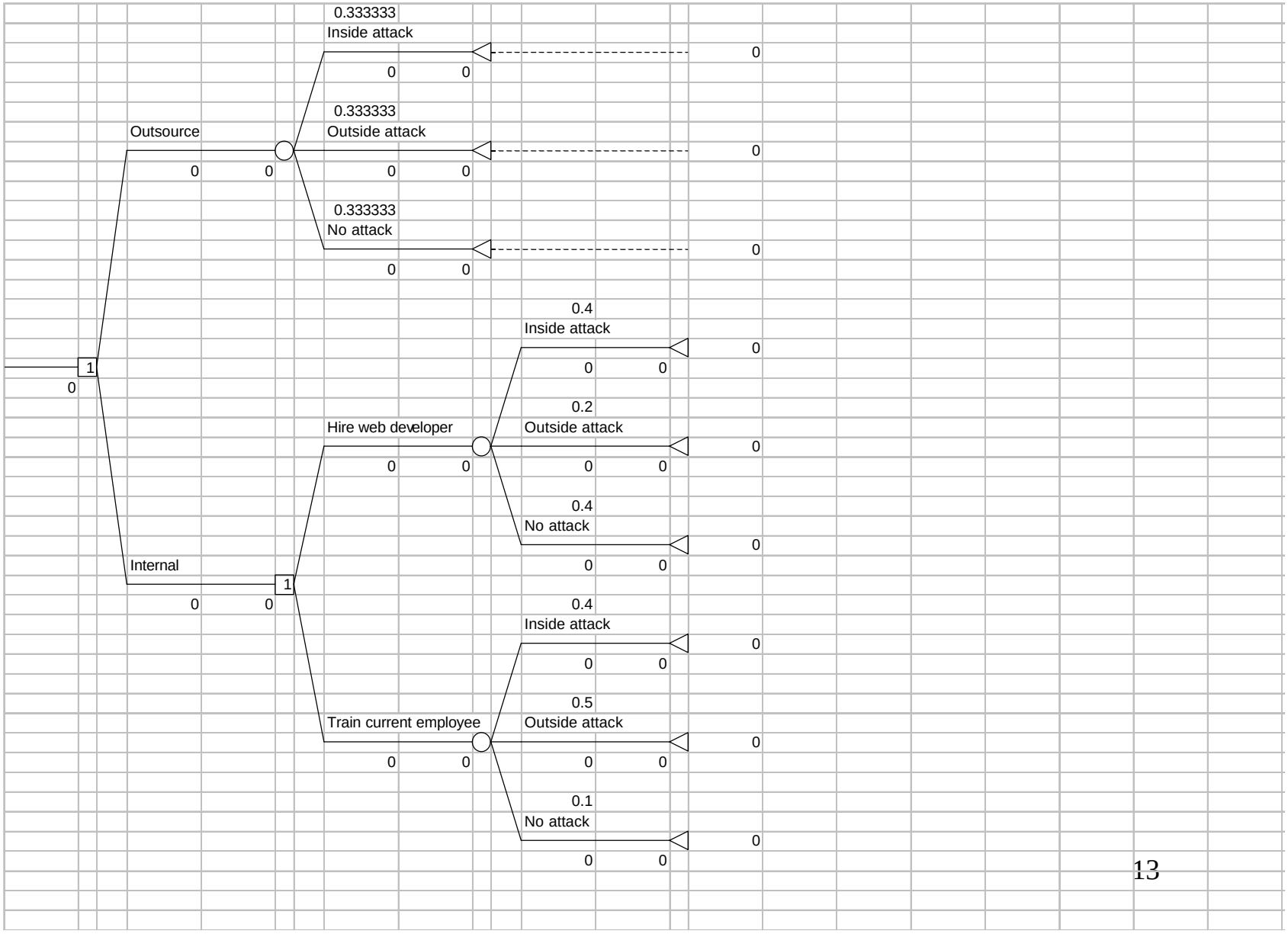
Financial Loss by Type of Attack and Size of Enterprise

A Decision Making Model for Securely Conducting Electronic Commerce

Decision	Inside Attack	Outside Attack	No Attack
Outsource	.33	.33	.33
Internal Hire	.4	.4	.2
Internal Train	.4	.5	.1

Probabilities of Attacks by Type of Attack by Decision

A Decision Making Model for Securely Conducting Electronic Commerce



Size of Enterprise	Cost of Single Inside Attack	Expected Value (Outsource)	Expected Value (Hire)	Expected Value (Train)	Optimal Decision
Small	10,000	22,000	78,000	104,000	Outsource
Medium	50,000	86,000	110,000	160,000	Outsource
Large	100,000	136,000	150,000	230,000	Outsource
Corporate	1,000,000	1,036,000	870,000	1,490,000	Hire

Secure Electronic Commerce Expected Value Matrix

Results

OUTSOURCE

Recommendations for Further Research

- Gather empirical data from small to medium size enterprises
- Determine the best security parameters to use for the model